The Odisha Gazette

EXTRAORDINARY
PUBLISHED BY AUTHORITY

No.1933, CUTTACK, WEDNESDAY, JULY 2, 2025/ASADHA 11, 1947

FISHERIES & ARD DEPARTMENT

NOTIFICATION

The 2nd July, 2025

No. 9375–FARD-MC-EGOV-0001/2025/FARD.– After careful consideration, the Government has been pleased to approve the Information Security Policy for the Fisheries & ARD Department, which needs to be implemented and maintained to protect information assets against unauthorized access that poses a substantial risk to the organization. The policy intends to establish adequate controls for user access management, network access, operating system security, and mobile computing in departmental processes and procedures.

ORDER

Order that the Notification be published in the next issue of the *Odisha Gazette*.

By Order of the Governor
S.K. VASHISHTH
Principal Secretary to Government

INFORMATION SECUTITY POLICY

Fisheries & ARD Department

Government of Odisha

Table of Contents

1. ACCESS CONTROL POLICY 4

1.1 Responsibility 4

1.2 Access Control Policy Statement and Objective 4

1.3 Privilege Management 4

1.4 Password Management Policy 4

2. COMMUNICATIONS AND OPERATIONS MANAGEMENT 5

2.1 Server Security Policy 5

2.2 Web Security Policy 5

2.3 Malicious code Management Policy 6

2.4 Configuration and Change Management Policy 6

2.5 Patch Management 7

2.6 Secure Logging and Privacy Controls 7

3. ASSET AND BACKUP MANAGEMENT POLICY 7

3.1 Introduction 7

3.2 Responsibility 7

3.3 Policy Statement and Objective 7

3.4 Personal Data Asset Management and Cloud Visibility 8

3.5 Information Classification 8

3.6 Information Labelling and Handling 8

3.7 Backup Management 9

4. INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE 9

4.1 Security Requirements of Information Systems 9

4.2 Cryptographic Controls 9

4.3 Security of System Files and Test Data 10

4.4 Security in Development and Support Processes 10

4.5 Technical Vulnerability Management 10

5. SECURITY MONITORING AND INCIDENT MANAGEMENT POLICY 10

5.1 Security Incident Management 10

6. COMPLIANCE POLICY 11

6.1 Regular Internal Security Audit for Security Policy compliance 11

6.2 Deliverables 9

1. ACCESS CONTROL POLICY

The Access Control Policy defines the controls that need to be implemented and maintained to protect information assets against unauthorized access that poses substantial risk to the organization. The policy intends to establish adequate controls for user access management, networks access, operating system security and mobile computing in departmental processes and procedures.

1.1 Responsibility

It is the responsibility of the IT and Networks department to implement and maintain the controls defined in the Access Control Policy and also the responsibility of the SIA / CT Designate to coordinate with the IT/ Networks department for User ID management controls.

1.2 Access Control Policy Statement and Objective

Access to information assets shall be controlled, based on the business and security requirements and commensurate with the asset classification. Access controls shall be deployed on the principle of 'deny all unless explicitly permitted' to protect the information from unauthorized access. The objectives of the Access Control Policy are to:

1. Restrict access to the information assets as per the departmental requirement;
2. Prevent unauthorized access to information systems, network services, operating systems and information held in database and application systems.
3. Ensure that the security controls are in place while using mobile computing and tele- working facilities;
4. Role-Based Access Control (RBAC) shall be implemented aligning with the principle of least privilege
5. Access reviews shall be performed quarterly to ensure appropriateness
6. Privacy by Design shall guide access controls to personal data

1.3 Privilege Management

Creation and allocation of privileged user accounts/ IDs on the information systems shall be controlled through a formal authorization process in accordance with the User Access Management Procedure.

1.4 Password Management Policy

Passwords are strings of characters that are input to a system to authenticate an identity and/or authority and/or access rights. Password policy is to be enforced for all the resources of various sections of a department who are dealing with critical information. This will help to prevent unauthorized access into system and services.

2. COMMUNICATIONS AND OPERATIONS MANAGEMENT

This section ensures correct and secure operational processes, protecting network and data, planning and implementation, protecting against malicious software, protecting data in transit and upgrading patches.

2.1 Server Security Policy

The physical and logical access should be controlled and monitored for the Server Farm. Storage security is the group of parameters and settings that make storage resources available to authorized Departmental users and trusted networks - and unavailable to other entities. These parameters can apply to hardware, programming, communication protocols and organizational policy.

2.2 Web Security Policy

The Web Security Policy provides the directions to ensure that the external interface to public needs to be in completely secured zone. Public access to Departmental infrastructure / electronic information resources, whether hosted in Department servers or external Web servers, will be established, maintained and administered in a secure environment.

Some of the standard practices in web security related avenues are captured below.

2.2.1 Responsibility

The Composite Team will define the appropriate controls and responsible officers have to implement ensuring against vulnerabilities in the web security. All applications hosted byFisheries & ARD Department shall be hosted as per security policy and public using the web systems of department are required to adhere to the Web Security Policy.

2.2.2.Policy Statement and Objective

The World Wide Web provides valuable information to the Internet community. However, there are security risks associated with providing such services. The Web Sites could be at risk to intruders who use the Internet as a means for attacking systems and causing various forms of threat. Consequently, Internet sites are often prime targets for malicious activity including break in, file tampering, and service disruptions. Such activity may be difficult to discover and correct, may be highly embarrassing to the organization, and can be very costly in terms of lost productivity and compromised data integrity. The purpose of this policy is to provide necessary standards to give guidance for the usage of publicly available methods of access such as the Internet, to Department’s information resources.

2.3 Malicious code Management Policy

Maintain a centralized Anti-Virus Management policy throughout.

2.4 Configuration and Change Management Policy

Potential impact of any change should be assessed before accepting a change request and Key changes should be authorized and documented by Departmental Project manager.

1. Suitable version control and a change log/directory should be maintained.

2. Concerned persons/practitioners should be intimated before implementation of a Change.
3. Process should be in place for recovering from 'unsuccessful' changes.
4. Changes to operational software such as Operating system upgrade, operating system changes, any application module upgrade, Vendor supplied software, Product enhancements, recommended patches should be controlled through change management procedure.
5. All approved changes should be maintained in Approved change management template.
6. Changes should be planned and access should be given to only those systems essential to carry out the work.
7. Environment for carrying out the tests should be separated from production and changes should be documented.
8. Any major changes to operating systems should be a planned activity and appropriate reviews should be done before implementation.
9. Authorized users from responsible team who can request changes and also the approval mechanism for a change request should be defined.
10. In case of version upgrades of operating systems through patches or software changes, the application should be tested fully for its functionality.
11. Modifications to Vendor Supplied products should be discouraged. If changes are warranted, vendors should be intimated to obtain system patches/releases and care should be taken that safety, functionality features are not getting impacted. The original software should be retained, and changes should be clearly documented.

2.5 Patch Management

Patches to the production systems shall be applied in a timely manner to ensure that the systems are running at their optimum level and threats from the spread of viruses, worms and malicious activities are reduced to an acceptable level. A formal Patch Management Procedure shall be established for applying patches to the information systems. All the critical patches that could affect the configuration of the critical information systems shall be subject to the Change Management Process.

2.6 Secure Logging and Privacy Controls

All operational technologies and cloud services shall implement secure baseline configurations.Event logs shall be generated and retained to support threat detection and privacy compliance.

3. ASSET AND BACKUP MANAGEMENT POLICY

3.1 Introduction

The Asset Management Policy specifies the importance of information assets including identification of the asset owner, asset classification and determining confidentiality,

integrity and availability ratings of the assets. The policy establishes the requirement of controls that need to be implemented for protecting information assets.

3.2 Responsibility

It is the responsibility of the Head of Department (HOD) of each department that owners are identified for all the information assets belonging to his/ her department and ownership is assigned to them. The asset owners are responsible for identifying, classifying, labeling and ensuring the protection of their respective information assets as per the Asset Management Procedure. The asset owner is also responsible for identifying the asset custodians for the assets under his/ her ownership. The asset custodians are responsible for the implementation of the required controls for the protection of information assets. All employees and third party staff are responsible for handling information assets as per the classification of the asset.

3.3 Policy Statement and Objective

Information assets of department shall receive comprehensive protection and shall have an identified owner. The objectives of the policy are to ensure that:-
An information asset register documenting the types of information assets of each business Department is maintained;

The information assets of each business Department have designated owners and custodians; and The CIA (Confidentiality, Integrity and Availability) ratings of information assets are ascertained.

3.4 Personal Data Asset Management and Cloud Visibility

1. Maintain a record of personal data assets, their processing purpose, and applicable data subjects.
2. Implement a cloud asset inventory system to track virtual resources and ownership (CSA AIS-01).

3.5 Information Classification

The information has different degrees of sensitivity and criticality to the business. The information classification categories shall be used to define an appropriate level of **protection or special handling**. The classification of the information needs to be consistent with the requirement and takes into account ‘Confidentiality’, ‘Integrity’ and ‘Availability’ ratings of the information. Information shall be classified in terms of its:

1. **Value**
2. **Legal Requirements**
3. **Sensitivity**
4. **Criticality**

The classification of information applies to information that is specifically meant for employees of the department. While its unauthorized disclosure is against the policy, it is not expected to seriously or adversely impact the business, employees, customers, stockholders and/ or business partners.

For information that is classified as ‘Restricted’ or ‘Confidential’, an assessment shall be done to identify the business, legal and/ or regulatory requirements for ascertaining its expected retention period.

3.6 Information Labelling and Handling

An appropriate set of procedures for information labeling and handling needs to be maintained and implemented in accordance with the information classification. For each classification level, the handling including its secure processing, storage, transmission and destruction have been defined in the Information Labeling and Handling Procedure.

3.7 Backup Management

1. Information owner in conjunction with System Administrator/NOC Team should identify the critical Server resources at Fisheries & ARD Departmentthat need to be backed up.

2. Appropriate backup media should be chosen by Information owner based on the criticality of data and retention period.

3. Periodicity of backup (backup schedule) should be determined by Information owner and the backups of Critical server resources should be taken by System Administrator/ NOC Team as per the schedule.

4. All backup media should be labeled as per the labeling convention detailed in department backup procedures.

5. Backup logs should be regularly maintained and kept up-to-date and it can be in the form of hard or softcopies

6. All backed-up resources should be stored in safe (fire-proof cabinet s) and protected place.

7. Backed-up data should be checked for its integrity and effectiveness through restoration of selective data.

8. Backup/Retrieval logs should be reviewed by the respective system administrator to ensure proper backup.

9. Sealed envelopes with signature should be used for transporting media to identified off-site location.

4. INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE

4.1 Security Requirements of Information Systems

Ensure that security is an integral part of information systems by the identification of all security requirements for the development and/or implementation of the information system. This policy applies to all new and existing ‘in scope’ information systems associated with the information processing facilities of the department and the responsible

personnel involved in development, maintenance and/or acquisition of information systems for the department.

4.2 Cryptographic Controls

Protect the confidentiality, authenticity and/or integrity of information by cryptographic means. Cryptographic controls shall be used to secure sensitive information of the ABC. A suitable strong encryption mechanism shall be used, based on the sensitivity of the information.

4.3 Security of System Files and Test Data

Control access to system files, program source code, and test data to ensure security of the same.

This policy applies to all Users of the ABC, who have access and usage rights to the ABC assets / resources and to all ABC Information Assets.

4.4 Security in Development and Support Processes

1. Control the ABC environment to ensure security of application system software and information.
2. All software development must include secure coding practices and regular code reviews.
3. Conduct privacy impact assessments (PIAs) for new systems processing personal data

4.5 Technical Vulnerability Management

Reduce the risks resulting from exploitation of published technical vulnerabilities.

5. SECURITY MONITORING AND INCIDENT MANAGEMENT POLICY

Incident management responsibilities and procedures will be established to ensure quick, effective and orderly response to security incidents. Incident management procedures will cover all types of potential security incidents, including the following:

1. Information System failure and loss of service due to security breaches or incidents.
2. Unauthorized access to the Departmental network
3. Deliberate denial of service
4. Wide-spread Virus or Worm outbreaks or Server infections.
5. Confidentiality breaches

5.1 Security Incident Management

Security incident should be defined as

1. Disruption of Departmental services
2. Modification of information /data related to department.
3. Sensitive information lost
4. Violation to Departmental policies
5. Unauthorized access to information

6. Identity thefts
7. Loss of Department/client's asset
8. Misuse of information & Computing resources
9. Incidents related to Physical security such as but not limited to, laptop lost, unauthorized entry into premises, assault
10. Define thresholds and alerting mechanisms for data breach events involving PII.
11. A cross-functional incident response plan must be tested annually, ensuring roles, escalation, and legal obligations are known.

6. COMPLIANCE POLICY

The operation and management of the Fisheries & ARD Department will be subject to statutory, regulatory and contractual requirements. Appropriate policies should be defined and followed to ensure such compliance. The objective for ensuring compliance is to avoid breaches of any criminal and civil law, and statutory, regulatory or contractual requirements.

6.1 Regular Internal Security Audit for Security Policy compliance

Departmental Security audit constitutes both technical and process audits, Technical audits are used to inspect the configuration of systems and examination of network to check whether they are in compliance. This is made possible by the usage of Tools, Scripts, Checklist and Snapshots. Audits of Process are performed to check whether processes for assurance of information security as mandated by the policies are being adhered to by the respective departments. The audits should be carried out as;

Planned Audit: Based on the risks perceived compliance Team should come up with the audit calendar. This calendar should indicate the organizations/locations that must get covered by the audits. Based on this calendar, Compliance schedules must be created. Draft Monthly Compliance schedules must be sent across to the Auditee and the Auditor and based on their feedback the final Compliance schedule must be published. Auditor should carry out the compliance check based on this schedule.

Unplanned Audit: Unplanned audits basically consist of Implementation checks and Spot- checks. Audit on implementation checks should be carried out on random basis. A schedule should be drawn and the auditee is informed about the same. The audit activity must happen immediately base on this schedule. Any new setup or any changes to the existing setup must be validated under this category on sample basis. All departments in the organization should be covered.

Audit Tracking and Reporting

All audits are individually tracked for closures and any significant audit exceptions are reported to the respective department head as well as to the Corporate Internal Audit Committee.

Audit findings for Planned and Unplanned audits should be based on the type of Risks and auditor will classify the finding as High Risk, Medium Risk or Low Risk. Auditor must classify the findings as Non-compliance to the documented procedure or Inadequacy in the system.

Final audit report must be published to the Auditee after the completion and sign off of the Draft audit report.

Multi-Framework Compliance Registry and Privacy Audit Controls

Maintain a compliance registry mapping internal controls to ISO 27001, NIST CSF categories, CSA CCM, and ISO 27701 controls.

Conduct privacy audits to ensure data subject rights and lawful basis for processing are enforced.

6.2 Indicative Deliverables

Mentioned below are the deliverables from both Planned and Unplanned audits:

1. Compliance Report.
2. Compliance Report based on departmental request.
3. Best practices implementation across State departments.
4. Root Cause analysis report

Principal Secretary to Government

Printed and Published by the Director, Printing, Stationery and Publication, Odisha, Cuttack-10

OGP/SBP Ex.Gaz.1143-183+50